Unitary Dynamics for Quantum Codewords

Asher Peres*

Institute for Theoretical Physics
University of California
Santa Barbara, CA 93106

A quantum codeword is a redundant representation of a logical qubit by means of several physical qubits. It is constructed in such a way that if one of the physical qubits is perturbed, for example if it gets entangled with an unknown environment, there still is enough information encoded in the other physical qubits to restore the logical qubit, and disentangle it from the environment. The recovery procedure may consist of the detection of an error syndrome, followed by the correction of the error, as in the classical case. However, it can also be performed by means of unitary operations, without having to know the error syndrome.

Since quantum codewords span only a restricted subspace of the complete physical Hilbert space, the unitary operations that generate quantum dynamics (that is, the computational process) are subject to considerable arbitrariness, similar to the gauge freedom in quantum field theory. Quantum codewords can thus serve as a toy model for investigating the quantization of constrained dynamical systems.

1. Introduction

In *classical* communication and computing systems, logical bits, having values 0 or 1, are implemented in a highly redundant way by bistable elements, such as magnetic domains. The bistability is enforced by coupling the bit carriers to a dissipative environment. Errors may then occur, because of thermal fluctuations and other hardware imperfections. To take care of these errors, various correction methods have been developed [1], involving the use of redundant bits (that are implemented by additional bistable elements).

In *quantum* communication and computing, the situation is more complicated: in spite of their name, the logical "qubits" (quantum binary digits) are not restricted to the discrete values 0 and 1. Their value can be represented by any point on the surface of a Poincaré sphere. Moreover, any set of qubits can be in an *entangled* state: none of the individual qubits has a pure quantum state, it is only the state of all the qubits together that is pure [2].

*Permanent address: Technion—Israel Institute of Technology, 32 000 Haifa, Israel

The qubits of a quantum computer are materialized by single quanta, such as trapped ions [3]. Their coupling to a dissipative environment (which was the standard stabilizing mechanism for classical bits) is now to be avoided as much as possible, because it readily leads to decoherence, namely to the loss of phase relationships. Yet, disturbances due to the environment cannot be completely eliminated: e.g., even if there are no residual gas molecules in the vacuum of an ion trap, there still are the vacuum fluctuations of the quantized electromagnetic field, which induce spontaneous transitions between the energy levels of the ions. Therefore, error control is an essential part of any quantum communication or computing system.

This goal is much more difficult to achieve than classical error correction, because qubits cannot be read, or copied, or duplicated, without altering their quantum state in an unpredictable way [4]. The feasibility of quantum error correction, which for some time had been in doubt, was first demonstrated by Shor [5]. As in the classical case, *redundancy* is an essential element, but this cannot be a simple repetitive redundancy, where each bit has several identical replicas and a majority vote is taken to establish the truth. This is because qubits, contrary to ordinary classical bits, can be *entangled*, and usually they are. As a trivial example, in the singlet state of two spin-$\frac{1}{2}$ particles, each particle, taken separately, is in a completely random state. Therefore, comparing the states of spin-$\frac{1}{2}$ particles that belong to different (redundant) singlets would give no information whatsoever.

All quantum error correction methods [5–9] use several physical qubits for representing one logical qubit. These physical qubits are prepared in a carefully chosen, highly entangled state. None of these qubits, taken alone, carries any information. However, a large enough subset of them may contain a sufficient amount of information, encoded in relative phases, for determining and exactly restoring the state of the logical qubit, including its entanglement with the other logical qubits in the quantum computer.

In this article, I review the quantum mechanical principles that make error correction possible. (I shall not discuss how to actually design new codewords; the most efficient techniques involve a combination of classical coding theory and of the theory of finite groups.) Since quantum codewords span only a restricted subspace of the complete physical Hilbert space, the unitary operations that generate the quantum dynamical evolution (that is, the computational process) are subject to considerable arbitrariness. The latter is similar to the gauge freedom in quantum field theory. Quantum codewords can thus serve as a simple toy model for investigating the quantization of constrained dynamical systems, such as field theories with gauge groups.

2. Encoding and decoding

In the following, I shall usually consider codewords that represent a single logical qubit. It is also possible, and perhaps it may be more efficient, to encode several qubits into larger codewords. However, no new physical principles are involved in this, and the simple case of a single qubit is sufficient for illustrating these principles.

The quantum state of a single logical qubit will be denoted as

$$\psi = \alpha\,|0\rangle + \beta\,|1\rangle, \tag{1}$$

where the coefficients α and β are complex numbers. The symbols $|0\rangle$ and $|1\rangle$ represent any two orthogonal quantum states, such as "up" and "down" for a spin, or the ground state and an excited state of a trapped ion.

In a quantum computer, there are many logical qubits, typically in a collective, highly entangled state, and any particular qubit has no definite state. I shall still use the same symbol ψ for representing the state of the entire computer, and Eq. (1) could now be written as

$$\psi = |\alpha\rangle \otimes |0\rangle + |\beta\rangle \otimes |1\rangle, \tag{2}$$

where one particular qubit has been singled out for the discussion, and the symbols $|\alpha\rangle$ and $|\beta\rangle$ represent the collective states of all the other qubits, that are correlated with $|0\rangle$ and $|1\rangle$, respectively. However, to simplify the notation and improve readability, I shall still write the computer state as in Eq. (1). In the following, Dirac's ket notation will in general *not* be used for generic state vectors (such as ψ, α, β) and the $\otimes$ sign will sometimes be omitted, when the meaning is clear. Kets will be used only for denoting basis vectors such as $|0\rangle$ and $|1\rangle$, and their direct products. The latter will be labelled by binary numbers, such as

$$|9\rangle \equiv |01001\rangle \equiv |0\rangle \otimes |1\rangle \otimes |0\rangle \otimes |0\rangle \otimes |1\rangle. \tag{3}$$

In order to encode the qubit ψ in Eq. (1), we intoduce an auxiliary system, called *ancilla*,[1] initially in a state $|000\ldots\rangle$. The ancilla is made of n qubits, and we can use the mutually orthogonal vectors $|a\rangle$, with $a = 0,\, 1,\, \ldots\,,\, 2^n - 1$ (the number a being written in binary notation) as a basis for its quantum states. These labels are called *syndromes*, because, as we shall see, the presence of an ancilla state with $a \neq 0$ may serve to identify an error in the encoded state that represents ψ.

Encoding is a unitary transformation, E, performed on a physical qubit and its ancilla together:

$$|z\rangle \otimes |a=0\rangle \to E\left(|z\rangle \otimes |a=0\rangle\right) \equiv |Z_0\rangle, \tag{4}$$

where $|z\rangle$ means either $|0\rangle$ or $|1\rangle$. This unitary transformation is executed by a quantum circuit (an array of quantum gates). However, from the theorist's point of view, it is also convenient to consider $|z\rangle \otimes |a=0\rangle$ and $|Z_0\rangle$ as two different representations of the same qubit $|z\rangle$: its logical representation, and its physical representation. The first one is convenient for discussing matters of principle, such as quantum algorithms, while the physical representation is the one where qubits are actually materialized by distinct physical systems (and the latter are the ones that may be subject to independent errors).[2]

[1] This is the Latin word for housemaid.

[2] These two different representations are analogous to the use of normal modes vs. local coordinates for describing the small oscillations of a mechanical system [10]. One description is mathematically simple, the other one is related to directly accessible quantities.

3. Error correction

If there are 2^n syndromes (including the null syndrome for no error), it is possible to identify and correct up to $2^n - 1$ different errors that affect the physical qubits, with the help of a suitable decoding method, as explained below. Let $|Z_a\rangle$, with $a = 0, \ldots ,$ $2^n - 1$, be a complete set of orthonormal vectors describing the physical qubits of which the codewords are made: $|0_0\rangle$ and $|1_0\rangle$ are the two error free states that represent $|0\rangle$ and $|1\rangle$, and all the other $|0_a\rangle$ and $|1_a\rangle$ are the results of errors (affecting one physical qubit in the codeword, or several ones, this does not matter at this stage). These $|Z_a\rangle$ are defined in such a way that $|0_a\rangle$ and $|1_a\rangle$ result from the *same* errors in the physical qubits of $|0_0\rangle$ and $|1_0\rangle$ (for example, the third qubit is flipped). We thus have two complete orthonormal bases, $|z\rangle \otimes |a\rangle$ and $|Z_a\rangle$. These two bases uniquely define a unitary transformation E, such that

$$E\left(|z\rangle \otimes |a\rangle\right) = |Z_a\rangle, \tag{5}$$

and

$$E^\dagger\,|Z_a\rangle = |z\rangle \otimes |a\rangle, \tag{6}$$

where a runs from 0 to $2^n - 1$. Thus, E is the encoding matrix, and $E^\dagger$ is the decoding matrix. If the original and corrupted codewords are chosen in such a way that E is a real orthogonal matrix (not a complex unitary one), then $E^\dagger$ is the transposed matrix, and therefore E and $E^\dagger$ are implemented by the *same* quantum circuit, executed in two opposite directions. (If E is complex, the encoding and decoding circuits must also have opposite phase shifts.)

The $2^n - 1$ "standard errors" $|Z_0\rangle \to |Z_a\rangle$ are not the only ones that can be corrected by the $E^\dagger$ decoding. Any error of type

$$|Z_0\rangle \to U\,|Z_0\rangle = \sum_a c_a\,|Z_a\rangle, \tag{7}$$

is also corrected, since

$$E^\dagger \sum_a c_a\,|Z_a\rangle = |z\rangle \otimes \sum_a c_a\,|a\rangle, \tag{8}$$

is a direct product of $|z\rangle$ with the ancilla in some irrelevant corrupted state. Note that *no knowledge of the syndrome is needed* in order to correct the error [11]. Error correction is a logical operation that can be performed automatically, without having to execute quantum measurements. We know that the error is corrected, even if we don't know the nature of that error.

It is essential that the result on the right hand side of (8) be a direct product. Only if the new ancilla state is the same for $|z\rangle = |0\rangle$ and $|z\rangle = |1\rangle$, and therefore also for the complete computer state in Eq. (2), is it possible to coherently detach the ancilla from the rest of the computer, and replace it by a fresh ancilla (or restore it to its original state

$|a=0\rangle$ by a dissipative process involving still another, extraneous, physical system).[3] This means, in the graphical formalism of quantum circuits, that the "wires" corresponding to the old ancilla stop, and new "wires" enter into the circuit, with a standard quantum state for the new ancilla.

There are many plausible scenarios for the emergence of coherent superpositions of corrupted states, as in (8). For example, in an ion trap, a residual gas molecule, whose wave function is spread over a domain much larger than the inter-ion spacing, can be scattered by all the ions, as by a diffraction grating, and then all the ions are left in a collective recoil state (namely, a coherent superposition of states where one of the ions recoiled and the other ones did not). Furthermore, *mixtures* of errors of type (8) are also corrigible. Indeed, if

$$\rho=\sum_j p_j \sum_{ab} c_{ja}\,|Z_a\rangle\,\langle Z_b|\,c^*_{jb}, \tag{9}$$

with $p_j>0$ and $\sum p_j=1$, then

$$E^\dagger\rho\,E=|z\rangle\,\langle z|\otimes\sum_j p_j \sum_{ab} c_{ja}\,|a\rangle\,\langle b|\,c^*_{jb}, \tag{10}$$

again is a direct product of the logical qubit and the corrupted ancilla.

These mixtures include the case where a physical qubit in the codeword gets entangled with an unknown environment, which is the typical source of error. Let η be the initial, unknown state of the environment, and let its interaction with a physical qubit cause the following unitary evolution:

$$\begin{aligned} |0\rangle\otimes\eta &\;\to\; |0\rangle\otimes\mu+|1\rangle\otimes\nu,\\ |1\rangle\otimes\eta &\;\to\; |0\rangle\otimes\sigma+|1\rangle\otimes\tau, \end{aligned} \tag{11}$$

where the new environment states $\mu,\ \nu,\ \sigma$, and τ, are also unknown, except for unitarity constraints. Now assume that the physical qubit, that has become entangled with the environment in such a way, was originally part of a codeword,

$$|Z_0\rangle=|X_{z0}\rangle\otimes|0\rangle+|X_{z1}\rangle\otimes|1\rangle. \tag{12}$$

That codeword, together with its environment, thus evolve as

$$Z_0\otimes\eta\to Z'=X_{z0}\otimes\Big(|0\rangle\otimes\mu+|1\rangle\otimes\nu\Big)+X_{z1}\otimes\Big(|0\rangle\otimes\sigma+|1\rangle\otimes\tau\Big), \tag{13}$$

where I have omitted most of the ket signs, for brevity. This can be written as

$$\begin{aligned} Z' \;=\; &\Big[X_{z0}\otimes|0\rangle+X_{z1}\otimes|1\rangle\Big]\,\frac{\mu+\tau}{2}+\Big[X_{z0}\otimes|0\rangle-X_{z1}\otimes|1\rangle\Big]\,\frac{\mu-\tau}{2}+\\ &\Big[X_{z0}\otimes|1\rangle+X_{z1}\otimes|0\rangle\Big]\,\frac{\nu+\sigma}{2}+\Big[X_{z0}\otimes|1\rangle-X_{z1}\otimes|0\rangle\Big]\,\frac{\nu-\sigma}{2}\,. \end{aligned} \tag{14}$$

[3] The introduction of a dissipative process in the quantum computer, which essentially is an analog device with a continuous evolution, brings it a step closer to a conventional digital computer!

On the right hand side, the vectors

$$\begin{aligned} Z_0 &= X_{z0}\otimes|0\rangle + X_{z1}\otimes|1\rangle,\\ Z_r &= X_{z0}\otimes|0\rangle - X_{z1}\otimes|1\rangle,\\ Z_s &= X_{z0}\otimes|1\rangle + X_{z1}\otimes|0\rangle,\\ Z_t &= X_{z0}\otimes|1\rangle - X_{z1}\otimes|0\rangle, \end{aligned} \tag{15}$$

correspond, respectively, to a correct codeword, to a phase error ($|1\rangle \to -|1\rangle$), a bit error ($|0\rangle \leftrightarrow |1\rangle$), which is the only classical type of error, and to a combined phase and bit error. If these three types of errors can be corrected, we can also correct any type of entanglement with the environment, as we shall soon see.

For this to be possible, it is necessary that the eight vectors in Eq. (15) be mutually orthogonal (recall that the index z means 0 or 1).[4] The simplest way of achieving this is to construct the codewords $|0_0\rangle$ and $|1_0\rangle$ in such a way that the following scalar products hold:

$$\langle X_{zy}\,,\,X_{z'y'}\rangle = \tfrac{1}{2}\,\delta_{zz'}\,\delta_{yy'}. \tag{16}$$

(There are 10 such scalar products, since each index in this equation may take the values 0 and 1.) If these conditions are satified, the decoding of Z' by $E^\dagger$ gives, by virtue of Eq. (6),

$$E^\dagger\,Z' = |z\rangle\otimes\left(|a=0\rangle\otimes\frac{\mu+\tau}{2} + |r\rangle\otimes\frac{\mu-\tau}{2} + |s\rangle\otimes\frac{\nu+\sigma}{2} + |t\rangle\otimes\frac{\nu-\sigma}{2}\right). \tag{17}$$

The expression in parentheses is an entangled state of the ancilla and the unknown environment. We cannot know it explicitly, but this is not necessary: it is sufficient to know that it is the same state for $|z\rangle = |0\rangle$ or $|z\rangle = |1\rangle$, or any linear combination thereof, as in Eq. (1). We merely have to discard the old ancilla and bring in a new one.

How to construct codewords that actually satisfy Eq. (16), when *any* one of their physical qubits is singled out, is a difficult problem, best handled by a combination of classical codeword theory [1] and finite group theory. I shall not enter into this subject here. I only mention that in order to correct an arbitrary error in any one of its qubits, a codeword must have at least five qubits: each one contributes three distinct vectors, like Z_r, Z_s, and Z_t in Eq. (15), and these, together with the error free vector Z_0, make 16 vectors for each logical qubit value, and therefore $32 = 2^5$ in the total. Longer codewords can correct more than one erroneous qubit. For example, Steane's linear code [7], with 7 qubits, can correct not only any error in a single physical qubit, but also a phase error, $|1\rangle \to -|1\rangle$, in one of them, and a bit error, $|0\rangle \leftrightarrow |1\rangle$, in another one (check! $1 + 7\times 3 + 7\times 6 = 2^{7-1}$). A well designed codeword is one where the orthogonal basis $|Z_a\rangle$ corresponds to the most plausible physical sources of errors.

The error correction method proposed above, in Eq. (6), is conceptually simple, but it has the disadvantage of leaving the logical qubit $|z\rangle$ in a "bare" state, vulnerable to new

[4] There is a slight risk of confusion here, because the same symbol 0 refers to the bit-value 0, and to the error free state of a codeword. I see no way of circumventing this difficulty without causing further confusion.

errors that would be not be detected. It is therefore necessary to re-encode that qubit immediately, with another ancilla (or with the same ancilla, reset to $|a=0\rangle$ by interaction with still another system). A more complicated but safer method is to bring in a second ancilla, in a standard state $|b=0\rangle$, and have it interact with the complete codeword in such a way that

$$|Z_a\rangle \otimes |b=0\rangle \to |Z_0\rangle \otimes |b=a\rangle. \tag{18}$$

This is also a unitary transformation, which can be implemented by a quantum circuit. Note that now the unitary matrix that performs that error recovery is of order 2^{2n+1}, instead of 2^{n+1}.

Naturally, errors can also occur in the encoding and decoding process. More sophisticated methods can however be designed, that allow fault tolerant computation. An adaptive strategy is used, with several alternative paths for error correction. Most paths fail, because new errors are created; however, these errors can be detected, and there is a high probability that one of the paths will eventually lead to the correct result. As a consequence, the error correction circuits are able to correct old errors faster than they introduce new ones. There is then a high probability for keeping the number of errors small enough, so that the correction machinery can successfully deal with them [12].

4. Constrained dynamics

A quantum codeword is a redundant representation of a logical qubit by means of several physical qubits. Since quantum codewords span only a restricted subspace of the complete physical Hilbert space, the unitary operations that generate quantum dynamics (that is, the computational process) are subject to considerable arbitrariness. This is most easily seen with the logical representation, $|z\rangle \otimes |a=0\rangle$. A unitary transformation, $\mathbb{1} \otimes g$, where g acts solely on the ancilla's states, generates

$$(\mathbb{1} \otimes g) \Big(|z\rangle \otimes |a=0\rangle \Big) = |z\rangle \otimes \sum_a c_a \, |a\rangle. \tag{19}$$

This is a corrupted, but corrigible codeword. In the physical representation, this harmless unitary transformation becomes

$$G = E \, (\mathbb{1} \otimes g) \, E^\dagger. \tag{20}$$

The unitary matrices G are a representation (usually a reducible one) of the Un group. Consecutive applications of various transformations of this type merely convert one corrigible error into another corrigible error. These transformations do not mix the two complementary subspaces that represent the logical 0 and 1.

On the other hand, a genuine unitary transformation (one that is actually needed for the computation) is, in the logical representation, $\psi \to \psi' = (u \otimes \mathbb{1})\psi$. It is encoded into

$$U = E \, (u \otimes \mathbb{1}) \, E^\dagger, \tag{21}$$

for the physical representation. Thus, in summary, all the "legal" unitary transformations are of type $E\,(u\otimes g)\,E^\dagger$, for codewords that represent a single logical qubit.

For unitary transformations involving two logical qubits, the encoded representation, including the possibility of corrigible errors, is likewise

$$U_{12}=(E_1\otimes E_2)\,[u_{12}\otimes(g_1\otimes g_2)]\,(E_1^\dagger\otimes E_2^\dagger), \tag{22}$$

where u_{12} acts on the two logical qubits, and g_1 and g_2 act on their respective ancillas. (I am assuming here that each logical qubit is encoded separately, and that block coding is not used.) It is obvious that in unitary transformations of that type, the logical steps are not affected by the occurrence or evolution of corrigible errors.

Among these unitary transformations, there is a subgroup leaving the zero-syndrome ancilla invariant (such a subgroup is called the *little group* of the invariant state):

$$g\,|a=0\rangle=|a=0\rangle. \tag{23}$$

Let us now focus our attention on these transformations, that do not induce errors in correct codewords. They only modify corrupted codewords, while keeping them corrigible. We may imagine, if we wish, that error free codewords are stabilized by erecting around them a high potential barrier: conceptually, we add to the Hamiltonian a potential term, equal to zero for the legal codeword states, and to a large positive number for erroneous states. This artifice is similar to, but much simpler than, the use of the quantum Zeno effect, that was proposed by several authors as a way of reducing errors. It is actually not difficult to devise quantum circuits that act like a potential barrier (the only serious difficulty is that such a circuit must activate high frequency interactions with extraneous qubits, and the latter may themselves be subject to errors, and induce new ones).

In the logical basis, a "legal" (error free) state, $|z\rangle\otimes|a=0\rangle$, which is invariant under the little group of $|a=0\rangle$, is recognized as being orthogonal to all $|z'\rangle\otimes|a\neq 0\rangle$. This can be written as an orthogonality relation

$$\langle C_\alpha\,,\psi\rangle=0, \tag{24}$$

where C_α is any linear combination of the various $|z'\rangle\otimes|a\rangle$ with $a\neq 0$. There are $2(2^n-1)$ linearly independent C_α, that span the "illegal" subspace (including incorrigible errors). Let us normalize them by $\langle C_\alpha\,,C_\beta\rangle=\delta_{\alpha\beta}$. After a legal unitary evolution, $U\psi$ still is a legal state, and therefore

$$\langle C_\alpha\,,U\psi\rangle=0. \tag{25}$$

It follows that

$$U\,C_\alpha=\sum_\beta A_{\alpha\beta}(U)\,C_\beta, \tag{26}$$

where the matrices $A_{\alpha\beta}(U)$ are a unitary representation of U. (If all legal U are considered, that representation will not, in general, be irreducible.)

It is also possible to construct Hermitian *operators* that express the same constraints. Recall that the codewords are defined in a Hilbert space with 2^{n+1} dimensions. Now consider

$$M=\sum_{\alpha\beta}|C_\alpha\rangle\,M_{\alpha\beta}\,\langle C_\beta|, \tag{27}$$

where $M_{\alpha\beta}$ is any matrix of order $2(2^n-1)$. Any legal state obeys $M\psi=0$. Another constraint (for the same codeword) could be $N\psi=0$, where

$$N=\sum_{\alpha\beta}|C_\alpha\rangle\,N_{\alpha\beta}\,\langle C_\beta|, \tag{28}$$

and $N_{\alpha\beta}$ is any other Hermitian matrix. It is easily shown that

$$[M,N]=iP, \tag{29}$$

where P is still another Hermitian operator of the same type, and satisfies $P\psi=0$ for all legal states. Finally, we note that if there are many logical qubits in the quantum computer, its state obeys the nonlocal "spacelike" constraint equation

$$M_1\otimes N_2\otimes\cdots\;\psi=0, \tag{30}$$

where the various operators refer to different codewords.

These equations are not completely trivial. They are like those appearing in a quantum field theory with a gauge group. For example, the canonical momenta of the free electromagnetic field are $\pi^k=E^k$, where $\mathbf{E}$ is the electric field vector. They satisfy the constraint $\partial_k\pi^k=0$. This cannot hold as an operator equation, because $\partial_k\pi^k$ does not commute with some other field operators. However, a legal state vector (one without "longitudinal photons") obeys the constraint $\partial_k\pi^k\psi=0$. The situation becomes more complicated for theories with non-Abelian gauge groups, such as general relativity: singular Schwinger terms appear, and the factor ordering problem cannot be discussed without regularization.[5]

An important problem in quantum field theory (or, in general, in quantum mechanics with constrained dynamical variables) is to properly define a Hermitian scalar product. Should we include in it the spurious particles that are generated by the gauge freedom, such as longitudinal photons? When we consider codewords, the situation becomes simple and clear, as we shall now see.

Consider indeed two different logical states of a quantum codeword, say

$$\varPhi=E\left(\phi\otimes\sum_a c_a\,|a\rangle\right), \tag{31}$$

and

$$\varPsi=E\left(\psi\otimes\sum_a c_a\,|a\rangle\right). \tag{32}$$

[5] For a recent review, see ref. [13].

On the left hand side, there is the physical representation of the codeword, and, in the parenthesis on the right hand side, its logical representation. Note that, irrespective of the logical state (ϕ or ψ), the ancilla has the same state $\sum c_a|a\rangle$, because that state represents the syndrome of the error, and the latter, caused by an interaction with the environment, is independent of the logical state of the qubit, as may be seen in Eq. (15). It then readily follows from the unitarity of E that the scalar products,

$$\langle \varPhi, \varPsi \rangle = \langle \phi, \psi \rangle, \tag{33}$$

are the same for any two non-orthogonal states of a logical qubit, and for their representation by codewords, even by corrupted ones. Further work is in progress, in order to exploit the analogies of quantum codeword dynamics with gauge field theory.

Acknowledgments

I am grateful to Peter Shor and Andrew Steane for clarifying remarks. This research was supported in part by the National Science Foundation under Grant No. PHY94-07194.

References

1. D. Welsh, *Codes and Cryptography*, Oxford University Press (1989), Chapt. 4.
2. A. Peres, *Quantum Theory: Concepts and Methods*, Kluwer, Dordrecht (1993), Chapt. 5.
3. J. I. Cirac and P. Zoller, Phys. Rev. Lett. 74 (1995) 4091.
4. W. K. Wootters and W. H. Zurek, Nature 299 (1982) 802.
5. P. W. Shor, Phys. Rev. A 52 (1995) 2493.
6. R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, Phys. Rev. Lett. 77 (1996) 198.
7. A. M. Steane, Phys. Rev. Lett. 77 (1996) 793; Proc. Roy. Soc. (London) in press.
8. C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A (in press).
9. E. Knill and R. Laflamme, “A theory of quantum error-correcting codes” (Los Alamos report LA-UR-96-1300).
10. H. Goldstein, *Classical Mechanics*, Addison-Wesley, Reading (1980), Chapt. 6.
11. A. Peres, Phys. Rev. A 32 (1985) 3266.
12. P. W. Shor, “Fault tolerant quantum computation” in *Proc. 37th Symposium on Foundations of Computer Science* (1996) in press. 830.
13. N. C. Tsamis and R. P. Woodard, Phys. Rev. D 36 (1987) 3641.